# Scam Calls - 10 Steps To Cyber-Safety

1
**Be sceptical of unknown callers**
If you don't recognise the number, let it go to voicemail.
Scammers often use call ID spoofing to make it look like a local or official number.

2
**Never share personal of financial information**
Do not give out your National Insurance number, credit card info,bank details or passwords over the phone. Legitimate organizations such as your bank, HMRC or the NHS will never ask for this unexpectedly

3
**Watch for urgent or threatening language**
Scammers often say things like: 'Your account will be frozen immediately!' or @You'll be arrested if you don't pay now!'.
Real organizations do not threaten or rush you like that.

4
**Do not pay with unsual methods**
Be suspicious if asked to pay with gift cards, cryptocurrency or wire transfers – these are hard to trace and are major red flags

5
**Hang up and verify**
If someone claims to be from your bank, HMRC, untility company or other known organization – Hang up and call the official number listed on their website or correspondence

6
**Register with the Telephone Preference Service**
Add your phone number to the Telephone Preference Service at tpsonline.org.uk. It will reduce unwanted marketing calls including scams.

7
**Trust your instincts**
If something seems off – it probably is, so hang up.
Don't let politeness or curiosity override your caution
Always remember that you control the conversation, not the caller.

8
**Use call-blocking tools**
Many phones and mobile networks offer call filtering or spam detection. Try services like BT Call Protect, Sky Talk Shield, or apps like Truecaller or Hiya.

9
**Help protect others**
Educate elderly family members or vulnerable friends = They are frequent targets. Encourage them to pause and verify before acting.

10
**Report scam calls**
Report scam calls to Action Fraud at actionfraud.police.uk or call 0300 123 2040. You can also report suspicious texts by forwarding them to 7726, free of charge.

# Reducing Your Cyber Fraud Risk

## Use strong, unique passwords

Use different passwords for every account
Consider using a password manager
to store your passwords securely

## Enable multi-factor authentication

Use two or more verification factors
to gain access to an account or system
e.g. Password+phone or Security key+fingerprint


## Be wary of phishing attempts

Don't click on links or attachments
in suspicious emails or messages

## Secure your devices and network

Keep your devices iupdated.
Secure your wi-fi and network with
strong passwords

## Monitor financial accounts regularly

Check bank and credit card statements
frequently for unauthorised activity

## Limit personal information shared online

Use privacy settings to control
who can see your social media posts.
Consider using a VPN


## Be cautious when shopping online

Only shop on secure sites.
Look for **https://** and a
padlock icon


## Shred sensitive documents

Shred documents like bank statements,
Medical information or any other paperwork
containing confidential data